DEPARTMENT OF ACCOUNTING AND GENERAL SERVICES
ANNUAL REPORT ON GOALS, OBJECTIVES AND POLICIES

January 2012

Program ID/Title: AGS-131/Information Processing & Communication Services

Contact Person/Phone: Debra A. Gagne/586-1910

The goals and objectives stated in this report are long-termed and are not limited by the existing budget. It charts a direction to improve the efficiency and effectiveness of State operations through the application of technology. Additional funding and resources will be needed to accomplish all of the goals and objectives contained herein. The Division's priority is to support, maintain, and improve existing services. We will accomplish as many of the goals and objectives as possible within the budget and resources granted.

I. Goals

Assess and redefine ICSD's services to support the State's current and future business requirements. Emphasis will be placed on the cost-effective and efficient application of information and telecommunications technologies to improve the long-term effectiveness and efficiency of Hawai'i State Government (State).

II. Objectives and Policies

A. #1 – Work with Chief Information Officer (CIO) and Office of Information Management and Technology (OIMT) to mitigate the risk of a $1,000,000 per day financial impact[1] to the State of Hawai'i resulting from lost revenues, collections, interest, late payments, overtime premiums and other costs that would be realized by the State as the result of a prolonged outage at the State of Hawai'i Data Center by establishing and operating an interim Alternate Data Center that will be utilized if a disaster were to occur at the Data Center at the Kalanimoku Building before a permanent data center co-located with the new State Emergency Operations Center (EOC) is operational.

B. #2 – Work with CIO and OIMT to develop and implement Service Oriented Architecture (SOA) as the State's information technology (IT) architecture and Information Technology Infrastructure Library ITIL/ IT Service Management Framework as the State's IT service delivery model.

[1] Estimated based on Business Impact Assessment conducted by McGladry, Inc. in February, 2002.

C. #3 - Work with CIO and OIMT to establish and operate a State Cyber Security Office with dedicated staff to provide statewide monitoring, analysis, prevention, and mitigation of cyber traffic to and from State information assets and resources. The major functions of this Office are to monitor and analyze State cyber traffic for cyber threats; provide preventive and remedial support against cyber threats; develop and implement an official notification and incident collection system; develop cyber security policies, standards, and procedures; coordinate with cyber security information sharing organizations; and other related matters.

D. #4 - Work with CIO and OIMT to improve the management and operation of the State's servers through the application of server consolidation technologies such as virtualization and blades.

E. #5 – Work with CIO and OIMT to establish IT Governance to manage IT initiatives and projects in the State with enhancements such as up-to-date IT strategic plans, cross departmental cost evaluations, standards and guidelines, project management plans, and status reports.

F. #6 - Work with CIO and OIMT to define the roles and responsibilities of ICSD staff.

G. #7 - Work with CIO and OIMT to expand and support the State's telecommunications infrastructure to enable secured connectivity from State offices to host computers for the State's application systems, and provide staffing and support of the State's radio communication systems.

H. #8 – Work with CIO and OIMT to improve the use of Internet technologies for sharing information with the public, government agencies, and private sector. Develop and implement better content management and document management practices to improve the quality of the information being shared and enhance the capability to preserve essential records.

I. #9 - Accommodate changes in State Data Center technologies, practices, and workload growth, while maintaining reliability, cost-effectiveness, and efficiency.

## III. **Action Plan with Timetable**

A. Objective/Policy #1 – Work with CIO and OIMT to mitigate the risk of a $1,000,000 per day financial impact[2] to the State of Hawai'i. State of Hawai'i critical business processes are heavily dependent upon information technology. The State of Hawai'i is the only state we are aware of that does not have an alternate for its primary data center facility[3]. Business continuity strategies for virtually all State agencies require that computers and networks that perform their information processing functions are operational, reliable, and predictably available.

Critical health, safety, and other public services (including processing of employee payroll, government aid and benefits to its most needy citizens, tax collections, payments to vendors, etc.) will be severely jeopardized by a prolonged data center outage, rendering the State vulnerable to damaged reputation, potential legal action and public outcry.

The State of Hawai'i Data Center in the Kalanimoku Building is a single point of failure that is below ground and relies on antiquated electrical and cooling systems which are running at or above their rated capacity. Given the criticality to the ongoing operations of the State, our number one priority is to continue pursuing the establishment of the State's main permanent data center co-located with the proposed new State Emergency Operations Center (EOC) and convert the existing datacenter to assume backup responsibilities. It is felt that since both facilities (EOC and Data Center) require many of the same things like a secure building highly resistant to wind and rain, cooling, and electrical systems which continue to function in the event of failure of the public utilities, and strong, redundant communications capabilities, the State could save considerable funds by combining these two critical needs into one facility. An interim alternate recovery facility could be found within 24 months, while co-occupancy of a State EOC is now projected to be about 2014.

---

[2] Estimated based on Business Impact Assessment conducted by McGladry, Inc. in February, 2002.

[3] Excerpted from State of Hawai'i Disaster Recovery Assessment Report and Recommendations 16 November 2005 provided by Gartner Consulting.

1. Required Actions

   a. Work with CIO and OIMT to harden the existing data center to the extent possible to avoid outage scenarios, including data center facilities, storage, backup capacity, Internet service, DNS and connectivity.

   b. Work with CIO and OIMT to obtain funding for the Division's budget to cover annual operating costs of the Interim Alternate Data Center.

   c. Work with CIO and OIMT to locate suitable data center facilities in a State-owned building or through commercial lease for an Interim Alternate Data Center.

   d. Work with CIO and OIMT to establish and implement an interim Alternate Data Center.

   e. Work with CIO and OIMT to develop a design plan for the permanent data center at the new State EOC.

   f. Work with CIO and OIMT to coordinate a CIP budget request with the Department of Defense for the permanent data center at the new State EOC.

   g. Work with CIO and OIMT to establish and implement a permanent data center at the new State EOC as soon as possible.

2. Past Year Accomplishments

   a. Consulted with the University of Hawai'i (UH) to assure space will be set aside in new UH data center for digital offsite backup.

   b. Consulted with the Department of Education (DOE) to assure space will be set aside in new Lili'uokalani data center for ICSD use.

   c. Provided background and historical information to CIO and OIMT.

d. The ICSD was able to eliminate additional single points of failure for the State of Hawai'i Data Center by establishing a secondary communications and Domain Name Services hub in another building. While this will not protect the State of Hawai'i Data Center, it will provide for continuing Internet access and connectivity for all locations outside of the Kalanimoku Building.

3. One Year

a. The Division will continue to pursue the establishment and operation of the interim Alternate Data Center. The Division will work closely with the CIO and the OIMT on disaster recovery planning.

b. The Division was invited to partner with the Department of Defense in their efforts for a new State EOC that targeted 2012 for completion, pending construction funding. Funding was not received and 2014 is the new targeted completion date. The Division plans on creating a permanent data center at this site running as a dark site (primarily for equipment). The current data center at the Kalanimoku Building would then become the alternate data center. Either the interim Alternate Data Center or the current data center at the Kalanimoku Building would become a business operations control center possibly after the permanent data center at the new State EOC becomes operational. The business operations control center would provide remote management of the servers and remote printing capabilities.

c. The Division will continue to work with CIO and OIMT on locating a prospective site for the interim Alternate Data Center.

d. The Division will continue to work with CIO and OIMT on the development of a design plan for a permanent data center at the new State EOC.

4. Two Years – Continue working with CIO and OIMT on pursuing a permanent data center at the proposed new State EOC and an interim Alternate Data Center. More details will be developed when necessary and sufficient funding becomes available.

5. Five Years – Continue working with CIO and OIMT on pursuing a permanent data center at the proposed new State EOC and an interim Alternate Data Center. More details will be developed when necessary and sufficient funding becomes available.

B. Objective/Policy #2 – Work with CIO and OIMT to develop and implement Service Oriented Architecture (SOA) as the State's information technology (IT) architecture and Information Technology Infrastructure Library ITIL/ IT Service Management Framework as the State's information technology (IT) service delivery model. The SOA emphasizes a close business-IT alignment driven by business. The SOA is based on open standards and defines a processing environment that enables compatible and disparate application systems to interoperate. The SOA also allows for the reuse of repeatable services that are part of the State's business processes. ITIL and IT Service Management is the provision of quality customer service. This is achieved by ensuring that customer requirements and expectations are met at all times. The satisfaction of business and customer requirements is fundamental to the whole of ITIL and there are a number of key activities that are vital to the success of ITIL processes.

1. Required Actions

a. Work with CIO and OIMT to educate ICSD Management on the principles and fundamentals of ITIL and IT Service Management.

b. Work with CIO and OIMT to develop Service Catalog, Change Management, and Customer Request systems to promote customer ease of use for service requests as well as tracking and measuring metrics.

c. Work with CIO and OIMT to promote the development of a standardized information technology infrastructure (e.g., standardized services and technologies) that will facilitate the sharing of the State's IT resources, simplify the support of those systems, and reduce costs to the State.

d. Work with CIO and OIMT to acquire short-term professional services to assist in the research, development, and implementation of new services, technologies, and standards.

e. Work with CIO and OIMT to coordinate the addition, enhancement, and elimination of services, technologies, and standards with agencies.

f. Work with CIO and OIMT to develop services that are based on new technologies while reducing and/or eliminating dependency on "old" technologies.

g. Work with CIO and OIMT to ensure that the Division has in-house knowledge to maintain services and standards.

2. Past Year Accomplishments – Fourteen positions were approved during the 2011 Legislative Session to allow restoration of third shift computer operations 24/7/365, as well as to mitigate several critical resource shortages throughout the Division.

a. Completed additional Enterprise Services Bus redundancy with multiple Enterprise Services Bus appliances installed and configured to be the foundation for the SOA Information Exchange Models.

b. Continued to make progress in the elimination of services that are based on "old" technology, such as impact printers, reel-to-reel tape drives, and manual data entry.

c. Developed cyber security standards, policies, and procedures and coordinated the dissemination of cyber security information to ensure the integrity of the State's information and IT services.

d. Investigated the use of technologies, such as PDF (portable document format), to provide an alternative service to hard copy documents while reducing cost and going "green" (e.g., eliminate paper).

e. Continued to make progress in the implementation of a virtual server environment that will consolidate standalone servers, reduce space and electrical requirements, provide high-availability, and improve disaster recovery capabilities.

f. Implemented a virtual tape system (VTS) that improves data backup and recovery services while lowering operating costs.

3. One Year

a. Work with CIO and OIMT to expand current activities to establish ICSD as the common service provider for SOA developed services. Develop SOA Governance and Central Services policies.

b. Work with CIO and OIMT to develop change management and problem management policies, documentation and systems that cover the technology utilized throughout the Data Center.

c. Work with CIO and OIMT to identify areas that require IT Governance to insure that technology and the State's IT resources can be leveraged as cost effective and efficient services.

d. Work with CIO and OIMT to pursue necessary personnel actions such as justifying additional positions, filling vacancies, and redescribing existing positions to insure that the Division has in-house knowledge to maintain services and standards.

e. Work with CIO and OIMT to place the virtual server environment and virtual tape system into production.

f. Work with CIO and OIMT to continue to provide value added services to our customers.

g. Work with CIO and OIMT to create pilot projects to gain expertise in new technologies that can be leveraged to make State government more efficient and effective.

h. Work with CIO and OIMT to continue to evaluate provided services to ensure applicability, identify areas for improvement, and eliminate redundancy.

i. Work with CIO and OIMT to begin using technologies, such as PDF (portable document format), to provide an

alternative service to hard copy documents while reducing cost and going "green" (e.g., eliminate paper).

4. Two Years

   a. Work with CIO and OIMT to continue with implementation and expansion of SOA in the form of reusable services across jurisdictions.

   b. Work with CIO and OIMT to continue to establish our role as IT for the State of Hawai'i and provide agencies with reliable and cost efficient IT services.

   c. Work with CIO and OIMT to continue evaluation and refinement of the services provided by the Division.

   d. Work with CIO and OIMT to continue to investigate new technologies that will provide cost reducing and "green" alternatives to our existing services.

   e. Work with CIO and OIMT to build coalitions, remove obstacles, gather buy-in, and work with agencies to identify new services that would be advantageous for the State to develop.

   f. Work with CIO and OIMT to determine the amount of professional services that would be required to assist in the research, development, and implementation of new services, technologies, and standards.

5. Five Years – New services developed utilizing SOA published services in innovative ways.

C. Objective/Policy #3 - Work with CIO and OIMT on a State Cyber Security Office that is firmly established with dedicated staff to provide statewide monitoring, analysis, prevention, and mitigation of cyber traffic to and from State information assets and resources. The major functions of this Office are to monitor and analyze State cyber traffic for cyber threats; provide preventive and remedial support against cyber threats; develop and implement an official notification and incident collection system; develop cyber security policies, standards, and procedures; coordinate with cyber security information sharing organizations; and other related matters.

1. Required Actions

    a. Work with CIO and OIMT on the evaluation and implementation of adequate technology tools to provide monitoring, mitigation and remediation of cyber security events.

    b. Work with CIO and OIMT to develop standard operating procedures for the Cyber Security Office, including training for the staff.

    c. Work with CIO and OIMT to complete staffing and re-organization for the office.

2. Past Year Accomplishments

    a. Populated cyber security website, cybersecurity.hawaii.gov, with cyber security awareness information, newsletters, cyber advisories and resources, video public service announcements, toolkits, and posters.

    b. Created website for State of Hawai'i ArcSight customers. Customers can now obtain their reports and explanations of correlated events and view documentation on demand.

    c. Responded to and managed the remediation of cyber security breaches to State Procurement sites, resulting in the development of a new service to scan any State website for possible vulnerabilities.

    d. The email security appliance system processes incoming messages to the network and scanned an average of 3 million messages a month.

    e. Implemented security software technology blocked 90% of malicious software incidents. Malicious IP addresses totaling 266 were also blocked.

    f. Utilized wildcard SSL digital certificates for servers under the hawaii.gov and higov.net domains, secure file transfer integration allowing servers to be further secured to protect personal and confidential information at little cost.

g. Distributed statewide advisories relating to vulnerabilities and patch recommendations; departmental notifications relating to suspicious network or computer activities; departmental investigations of potential malicious cyber security events; and coordinated cyber incident remediation efforts.

h. Investigated potential malicious cyber security activity on the State network using ArcSight, a security information and event management tool, to follow up on alerts, security violations, copyright investigations, possible infected hosts, and attempted activity from previously-identified malicious IP addresses.

i. Implemented a vulnerability scanning program on ICSD public and internal servers to identify computer server and operating system vulnerabilities to assist server administrators to secure their server environment against computer threats.

j. Implemented a web application security testing tool to assist ICSD software developers to write secure web programming code to protect against web application vulnerabilities and cyber attacks.

k. Developed cyber security policies, standards, guidelines, and a security incident handling policy for ICSD which are available as guidelines for use by other departments.

l. Participated in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and InfraGard security organizations to foster information sharing and collaboration on cyber security threat prevention, protection, and response and recovery activities.

m. Implemented the Secure Web Gateway tool to block malicious or unwanted access to websites by name and not just IP address.

n. Participated in APEC preparations for the Multi-Agency Communications Center.

One Year - Continue current activities.

a. Provide cyber-security services as a requested service.

b. Implement the Secure Web Gateway to additional State Departments and agencies to block malicious or unwanted access to websites by name.

c. Migrate local area network, web servers, and application servers to a virtual environment.

4. Two Years – Work with CIO and OIMT to expand cyber security service offering to at least 10 more agencies.

5. Five Years – Work with CIO and OIMT to continue the development of cyber security standards, so that cyber security preparation, mitigation and remediation become standard practice across the State.

D. Objective/Policy #4 - Work with CIO and OIMT to improve the management and operation of the State's servers through the application of server consolidation technologies such as virtualization and blades.

1. Required Actions

a. Work with CIO and OIMT to research the various server consolidation technologies and evaluate their applicability to State operations.

b. Work with CIO and OIMT to pursue funding to proceed with server consolidation.

c. Work with CIO and OIMT to acquire and implement the selected technologies.

d. Work with CIO and OIMT to review the Division's technical support structure and revise as required.

2. Past Year Accomplishments

a. Built a virtual server environment. Procured several blade servers, accompanying disk storage, as well as virtualization software.

b. Created a cross division virtual server team to establish the virtual server environment and to develop plans to migrate stand alone server applications to a virtual server environment.

c. Provided training and development for the virtual server team in VMWare, MsSQL, Active Directory, and storage concepts in a virtual environment.

3. One Year

a. Work with CIO and OIMT to complete Active Directory and Domain Name Services (DNS) technology implementations to fully utilize the virtual environment.

b. Work with CIO and OIMT to evaluate server workload and migrate appropriate processing to virtual environment to reduce energy consumption in the State of Hawai'i Data Center, as well as freeing up data center floor space.

4. Two Year

Work with CIO and OIMT to promote "internal" Cloud infrastructure services to State departments and agencies to provide application independent processing, storage and networking in a highly available infrastructure environment.

5. Five Year
Continue to work with CIO and OIMT to consolidate department and agency specific infrastructure into the centrally managed and administered cloud infrastructure.

E. Objective/Policy #5 – Work with CIO and OIMT to establish IT Governance to manage IT initiatives and projects in the State with enhancements such as up-to-date IT strategic plans, cross departmental cost evaluations, standards and guidelines, project management plans, and status reports.

1. Required Actions

a. Work with CIO and OIMT to establish a consolidated planning process for IT initiatives and projects in the State,

utilizing the IT leadership provided by the IT Governance Committees.

b. Work with CIO and OIMT to establish a process to register IT initiatives and projects, monitor for compliance with State standards, and track progress.

c. Work with CIO and OIMT to establish a process to set or modify IT standards and guidelines.

d. Work with CIO and OIMT to develop a service to facilitate the implementation of IT initiatives and projects.

e. Work with CIO and OIMT to coordinate all of the above actions with the CIO.

2. Past Year Accomplishment - The IT Governance Technical Committees continued to meet on regular schedules. The ICSD continued to lead the Technical Committee. The Committee continued work on the IT Transition document for the CIO and state leadership

a. IT Governance Technical Committee evaluated consolidation strategies to mitigate the resource shortages created by the reduction-in-force.

b. When the Legislature is in session, tracking bills and resolutions take on a frenetic pace. To assist other departments in keeping current, the ICSD delivered a Lotus Notes-based Legislative Tracking System application to several departments.

c. Conducted strategic planning sessions with the IT technical Governance Committee.

3. One Year

a. Work with CIO and OIMT to identify areas requiring Statewide IT Governance to insure technology is leveraged and used in a cost effective and efficient manner.

b. Work with CIO and OIMT to draft revisions to the current policies and related documents including clarification of central and departmental roles.

c. Work with CIO and OIMT to re-engineer processes and evaluation of resources required, such as staffing and budgets to implement the policies that result from the revisions.

4. Two Years – Continue to work with CIO and OIMT on the evaluation and refinement of the processes and services.

5. Five Years – Continue to work with CIO and OIMT on the evaluation and refinement of the processes and services.

F. Objective/Policy #6 - Work with CIO and OIMT to define the roles and responsibilities of ICSD staff.

1. Required Actions

a. Work with CIO and OIMT to provide staff with training, tools, a standard infrastructure/environment, and support to perform their broadened roles.

b. Work with CIO and OIMT to acquire short-term professional services to assist the ICSD in the development of new systems. This will allow the ICSD to take on new development, ensure that the State has in-house knowledge to maintain the systems, and reduce the State's dependence on consultants for enhancement/maintenance services.

c. Work with CIO and OIMT to assess staff resource requirements and acquire as needed.

d. Work with CIO and OIMT to coordinate application development requirements and efforts with agencies.

e. Work with CIO and OIMT to make data more accessible to agencies (e.g., data mart), such that they will be empowered to retrieve data on their own.

2. Past Year Accomplishments

a. Progress stalled somewhat from previous year. Focus became keeping the important systems running. Staff took on a few small development projects and completed them successfully. Significant staff time was needed to make the programming modifications for payroll etc. to reflect the financial actions decided upon by State's leaders.

b. Training was limited to only no-cost training; therefore, most training was self-initiated, gleaned from industry trade journals or provided through State Civil Defense.

c. More advanced and diverse training is being researched and pursued. particularly as an online per-seat train on your time effort.

d. Continued Quarterly Customer Service Reports for all departments. These customer-focused reports detailed departmental resource utilization and provided current technology implementation information.

3. One Year

a. Work with CIO and OIMT to create activities to document work activities to assure transfer of institutional knowledge as staff left or retired.

b. Work with CIO and OIMT to pursue necessary personnel actions such as filling vacancies and redescribing positions.

c. Work with CIO and OIMT to acquire tools including computer software and reference books or services.

d. Work with CIO and OIMT to continue to provide added value maintenance services to our customers.

e. Work with CIO and OIMT to create pilot projects on development of new applications to gain expertise in new technologies.

f. Work with CIO and OIMT to retrofit existing systems to extend their lives, improve usability, and reduce maintenance requirements.

4. Two Years

   a. Work with CIO and OIMT and agencies in determining which systems would be advantageous for the State to develop. Begin the development process.

   b. Work with CIO and OIMT to determine the amount of professional services that would be required for the selected projects.

   c. Work with CIO and OIMT to continue to provide agencies with professional IT services.

   d. Work with CIO and OIMT to continue to develop the State's SOA environment.

   e. Work with CIO and OIMT to continue to retrofit existing systems.

5. Five Years – Work with CIO and OIMT to continue to provide staff with refresher training to remain current with changing technologies, standards, and methodologies. To be effective, as alternatives to private consultants, their knowledge and skill levels need to be kept near that of private consultants.

G. Objective/Policy #7 - Work with CIO and OIMT to expand and support the State's telecommunications infrastructure to enable secure connectivity from State offices to host computers for the State's application systems, and provide operational support of the State's radio communication systems.

1. Required Actions

   a. Ensure support to continue the operation and maintenance of the Hawai'i Wide Area Integrated Information Access Network (HAWAIIAN).

   b. Expand the use and enhance reliability and survivability of the NGN.

   c. Expand network connectivity to State offices and workstations.

d. Enhance and expand video capabilities for intrastate, interstate, and international communications.

e. Expand and enhance telephone services.

f. Provide a survivable, fault tolerant backbone for land mobile radio interconnection based on the HAWAIIAN.

g. Hire additional staff to support the statewide radio communications system that provides services, and supports the State's communication needs for public safety, emergency services, natural resource protection, and others.

2. Past Year Accomplishments

a. Increased bandwidth between NGN core switches.

b. Deployed security information management system capability to user departments.

c. Ānuenue IOC (Initial Operating Condition) was achieved and publicly announced September 30, 2008. Pursuing development of the Rescue21 program with the United States Coast Guard.

d. Migrated core network systems to a multi protocol layered system (MPLS) to provide a foundation for reducing costs by replacing distinct network configurations with shared bandwidth technology.

e. Proposals for State telephone system and long distance were awarded.

f. Provided an alternate route over the ICSD HAWAIIAN microwave for State Civil Defense's Round Top to Diamond Head payload.

g. Video Conferencing – Developed a partnering agreement with the Department of Land and Natural resources to expand Video Conferencing capability by 75%.

h. Partnered with user departments and agencies across the State and with Hawaiian Telecom to develop an easier to use Telecom Request Form which can now be

electronically filled and saved, greatly speeding ordering time.

i. SOHEM consolidated messaging - Implemented optional BlackBerry and iPhone support for email accounts residing on ICSD Domino Servers. Provided guidance to agencies in upgrading their messaging software. Reduced out-of-office notification period from six to two hours. Expanded anti-SPAM and anti-virus protection for all @hawaii.gov clients. Installed new statewide e-mail relay servers enabling agencies to mail enable their application processes.

3. One Year

a. Work with CIO and OIMT to continue to monitor the performance, functionality, and security of NGN. Make necessary adjustments to enhance its operation and meet requirements as they evolve.

b. Work with CIO and OIMT to continue to work with the counties to expand their connectivity to NGN to facilitate access to shared applications and services by State and county agencies.

c. Work with CIO and OIMT to continue working on development and construction of microwave sites for Anuenue System upgrade.

d. Work with CIO and OIMT to continue to seek and upgrade network monitoring capabilities for NGN and HAWAIIAN.

e. Work with CIO and OIMT to continue to enhance the network to provide greater reliability, security, and services.

f. Work with CIO and OIMT to continue maintenance of HAWAIIAN microwave sites, including structural and equipment repairs, upgrades, and enhancements.

g. Work with CIO and OIMT to continue to evaluate alternatives for a statewide radio communications system

for State agencies. Develop requirements for these alternatives.

h. Installation of a new generator at the Round Top microwave radio facility.

4. Two Years

a. Work with CIO and OIMT to continue establishing connectivity to NGN from State agencies and other government jurisdictions.

b. Work with CIO and OIMT to continue evaluating alternative ISP connections.

c. Work with CIO and OIMT to study and design of interoperability solution for public safety and emergency response radio systems.

d. Participant in initiatives to implement Broadband capability throughout the State.

5. Five Years - Work with CIO and OIMT to continue support, connectivity, and enhancement of the NGN depending on requirements and funding.

H. Objective/Policy #8 - Work with CIO and OIMT to improve the use of Internet technologies for sharing information with the public, government agencies, and private sector. Develop and implement better content management practices to improve the quality of the information being shared.

1. Required Actions

a. Work with CIO and OIMT to develop and implement new Internet technologies, tools, and methods to improve access to public information, and facilitate the State's communications with the citizenry, business, and other government jurisdictions.

b. Work with CIO and OIMT to continue to work and collaborate with the State's Internet Portal contractor to add more State e-commerce services for the public to access over the Internet.

2. Past Year Accomplishments

   a. Created a new look for the Office of the Governor website.

   b. Redesigned and upgraded the websites for the State Procurement Office.

   c. Continued to provide technical training and mentoring for support staff.

   d. Issued the Accessibility Policy and audited websites for compliance.

   e. Developed Social Media usage policy with cooperation of the Attorney General's Office.

3. One Year

   a. Work with CIO and OIMT to implement and migrate to server equipment acquired to increase the storage capacity of the State's web servers to accommodate more public information.

   b. Work with CIO and OIMT to provide technical training and mentoring for support staff to enable them to further develop the quality and content of the State's websites. Continue to work towards compliance with guidelines on access by the disabled.

4. Two Years – Monitor usage and make improvements and adjustments as needed.

5. Five Years – Monitor usage and make improvements and adjustments as needed.

I. Objective/Policy #9 - Work with CIO and OIMT to accommodate changes in State Data Center technologies, practices, and workload growth, while maintaining reliability, cost-effectiveness, and efficiency.

1. Required Actions

   a. Work with CIO and OIMT to implement a Business Continuity Plan for the Division.

b. Work with CIO and OIMT to expand network monitoring and support coverage to 24 hours per day, seven days a week, including holidays.

c. Work with CIO and OIMT to expand the automation of computer and network operation and management.

d. Work with CIO and OIMT to plan and implement alternative technologies for producing computer output reducing paper consumption.

e. Work with CIO and OIMT to plan and implement on-line production documentation.

f. Work with CIO and OIMT to lead user agencies in developing, implementing, and testing a statewide IT business continuity plan.

g. Work with CIO and OIMT to expand network monitoring to all networks in State government.

h. Work with CIO and OIMT to initiate discussions with various Executive Branch agencies to adopt business process re-engineering methods to streamline and increase efficiency to their operations while eliminating manual processes that require human interventions for the Data Center staff.

i. Work with CIO and OIMT on plan to reduce and eventually eliminate batch data entry operations.

j. Work with CIO and OIMT to initiate discussions with various program offices to convert current check printing operations to adopt electronic means of financial transactions.

2. Past Year Accomplishments

a. Finalized the elimination of antiquated microfilm and microfiche technologies.

b. Converted magnetic media input files to electronic File Transfer Protocols (FTP) increasing efficiency, accuracy, reliability and security.

3. One Year

a. Work with CIO and OIMT to continue working on the project to migrate computer output from printed to electronic media, and enabling secured on-line access to the repository.

b. Work with CIO and OIMT to continue working on the plan to provide expanded network monitoring services to departmental networks in the State.

c. Work with CIO and OIMT to continue updating position descriptions, recruiting, and filling positions within the Productions Services Branch. The recently approved reorganization will enable the Division to better support the disaster recovery and front-line server support functions.

d. Work with CIO and OIMT to continue to migrate LAN and server backups to a common backup solution, TSM (Tivoli Storage Manager).

4. Two Years

a. Work with CIO and OIMT to continue to lead user agencies in developing, implementing, and testing a statewide IT data center disaster recovery and business continuity plans.

b. Work with CIO and OIMT to continue work in developing, implementing, and testing a statewide IT data center disaster recovery and business continuity plan with other user agencies.

5. Five Years - Work with CIO and OIMT to continue evaluation of State requirements, and centralized operations for information processing, telecommunications services, and IT support.

## III. Performance Measures

A. Customer Satisfaction Measure – Work with CIO and OIMT to measure services based on using agreed upon metrics provided by customers. Evaluate service level agreements, MOU's and MOA's to ascertain adherence and to determine areas for improvement.

B. Cost Effectiveness Measure – Work with CIO and OIMT to determine how annual costs will be monitored as necessary.

Availability Reporting – a Root Cause Analysis Report and a corresponding Corrective Action Plan will be created for outages impacting customers with sign off by the impacted customer prior to closure.